PATENTS

#2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Kaoru Uchida

Examiner: Unassigned

Serial No: Unassigned

Art Unit: Unassigned

Filed: Herewith

Docket: 14098

For: USER AUTHENTICATION APPARATUS WHICH USES BIOMETRICS AND USER AUTHENTICATION METHOD FOR USE WITH USER AUTHENTICATION APPARATUS

Dated: November 27, 2000

Assistant Commissioner for Patents
United States Patent and Trademark Office
Washington, D.C. 20231

CLAIM OF PRIORITY

Sir:

Applicant in the above-identified application hereby claims the right of priority in connection with Title 35 U.S.C. § 119 and in support thereof, herewith submits a certified copy of Japanese Patent Application No. 11-348268, filed on December 8, 1999.

Respectfully submitted,

PJE

Paul J. Esatto, Jr.
Registration No.: 30,749

Scully, Scott, Murphy & Presser
400 Garden City Plaza
Garden City, New York 11530
(516) 742-4343

CERTIFICATE OF MAILING BY "EXPRESS MAIL"

Express Mailing Label No.: EL658969316US

Date of Deposit: November 27, 2000

I hereby certify that this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. § 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents and Trademarks, Washington, D.C. 20231 on.

Dated: November 27, 2000

Janet Giordano

Janet Giordano

ND-3665

JC853 U.S. PTO
09/722964
11/27/00

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年１２月 ８日

出 願 番 号
Application Number: 平成１１年特許願第３４８２６８号

出 願 人
Applicant (s): 日本電気株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年 ９月１８日

特 許 庁 長 官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３０７５７０９

【書類名】　特許願
【整理番号】　33509628
【提出日】　平成11年12月 8日
【あて先】　特許庁長官殿
【国際特許分類】　G06T 7/00
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　内田　薫
【特許出願人】
　【識別番号】　000004237
　【氏名又は名称】　日本電気株式会社
【代理人】
　【識別番号】　100088812
　【弁理士】
　【氏名又は名称】　▲柳▼川　信
【手数料の表示】
　【予納台帳番号】　030982
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　バイオメトリクスを用いるユーザ認証装置及びそれに用いるユーザ認証方法

【特許請求の範囲】

【請求項１】　個人に固有の生体特徴であるバイオメトリクスの照合でユーザを認証するバイオメトリクスを用いるユーザ認証装置であって、前記バイオメトリクスの照合で認証不可の時に当該認証を要求したユーザのバイオメトリクスデータを取得する取得手段と、前記取得手段で当該バイオメトリクスデータが取得された時に前記バイオメトリクスの照合を代替する代替認証手段とを有することを特徴とするユーザ認証装置。

【請求項２】　前記取得手段で取得したバイオメトリクスデータを保存する保存手段と、前記保存手段に保存されたバイオメトリクスデータに基づいて不正利用者探索及び追跡を行う処理手段とを含むことを特徴とする請求項１記載のユーザ認証装置。

【請求項３】　前記バイオメトリクスの照合を目的として入力されたバイオメトリクスデータが自動照合に適した品質であるか否かを判定する手段と、当該バイオメトリクスデータが自動照合に適した品質でないと判定された時にその取得されたバイオメトリクスデータを保存する手段とを含むことを特徴とする請求項１または請求項２記載のユーザ認証装置。

【請求項４】　前記バイオメトリクスデータが自動照合に適した品質でないと判定された時に当該バイオメトリクスデータが前記不正利用者探索及び追跡に用いるに適した品質であるか否かを判定する手段を含み、前記不正利用者探索及び追跡に用いるに適すると判定された時に前記代替認証手段の使用を許可するよう構成したことを特徴とする請求項３記載のユーザ認証装置。

【請求項５】　前記不正利用者探索及び追跡に用いるに適した品質であるか否かを判定する際に、入力されるバイオメトリクスデータが正しくそのユーザがその場で入力したものであるか否かの判断を用いるようにしたことを特徴とする請求項４記載のユーザ認証装置。

【請求項６】　前記取得手段で取得された複数のバイオメトリクスデータの相関を計測することで、そのユーザがその場で入力したものであるか否かの判断を行うようにしたことを特徴とする請求項５記載のユーザ認証装置。

【請求項７】　前記バイオメトリクスとして、少なくと指紋を用いるようにしたことを特徴とする請求項１から請求項６のいずれか記載のユーザ認証装置。

【請求項８】　前記代替認証に先立つバイオメトリクスデータ保存の際に、少なくと顔画像や指紋入力する姿を撮影するようにしたことを特徴とする請求項１から請求項７のいずれか記載のユーザ認証装置。

【請求項９】　個人に固有の生体特徴であるバイオメトリクスの照合でユーザを認証するバイオメトリクスを用いるユーザ認証方法であって、前記バイオメトリクスの照合で認証不可の時に当該認証を要求したユーザのバイオメトリクスデータを取得するステップと、当該バイオメトリクスデータが取得された時に前記バイオメトリクスの照合を代替する代替認証手段で代替認証を行うステップとを有することを特徴とするユーザ認証方法。

【請求項１０】　前記バイオメトリクスデータを取得するステップで取得したバイオメトリクスデータを保存するステップを含み、その保存されたバイオメトリクスデータに基づいて不正利用者探索及び追跡を行うようにしたことを特徴とする請求項９記載のユーザ認証方法。

【請求項１１】　前記バイオメトリクスの照合を目的として入力されたバイオメトリクスデータが自動照合に適した品質であるか否かを判定するステップと、当該バイオメトリクスデータが自動照合に適した品質でないと判定された時にその取得されたバイオメトリクスデータを保存するステップとを含むことを特徴とする請求項９または請求項１０記載のユーザ認証方法。

【請求項１２】　前記バイオメトリクスデータが自動照合に適した品質でないと判定された時に当該バイオメトリクスデータが前記不正利用者探索及び追跡に用いるに適した品質であるか否かを判定するステップを含み、前記不正利用者探索及び追跡に用いるに適すると判定された時に前記代替認証を許可するようにしたことを特徴とする請求項１１記載のユーザ認証方法。

【請求項１３】　前記不正利用者探索及び追跡に用いるに適した品質である

か否かを判定する際に、入力されるバイオメトリクスデータが正しくそのユーザがその場で入力したものであるか否かの判断を用いるようにしたことを特徴とする請求項１２記載のユーザ認証方法。

【請求項１４】　前記バイオメトリクスデータを取得するステップで取得された複数のバイオメトリクスデータの相関を計測することで、そのユーザがその場で入力したものであるか否かの判断を行うようにしたことを特徴とする請求項１３記載のユーザ認証方法。

【請求項１５】　前記バイオメトリクスとして、指紋を用いるようにしたことを特徴とする請求項９から請求項１４のいずれか記載のユーザ認証方法。

【請求項１６】　前記代替認証に先立つバイオメトリクスデータ保存の際に、少なくと顔画像や指紋入力する姿を撮影するようにしたことを特徴とする請求項９から請求項１５のいずれか記載のユーザ認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はバイオメトリクスを用いるユーザ認証装置及びそれに用いるユーザ認証方法に関し、特にゲート等における物理的アクセス管理やパーソナルコンピュータ等の端末での情報アクセス管理の際に指紋等のバイオメトリクスでユーザ本人を認証する方法に関する。

【０００２】

【従来の技術】

従来、ユーザ認証方法においては、入門ゲート等における物理的アクセス管理やパーソナルコンピュータ等の端末での情報アクセス権の管理を行うユーザが本人かどうかを確認するために用いられている。

【０００３】

このユーザ認証方法では磁気カード等の所持品を持っているか否か、あるいは暗証番号やパスワード等の秘密知識を知っているか否かによって認証を行う方法に加えて、バイオメトリクスによる認証が使用されている。

【０００４】

バイオメトリクスとは指紋等の個人毎に特有な生体特徴を利用するものである。人間の指先の皮膚紋様である指紋は「万人不同」や「終生不変」という特徴を持つとされ、表皮が損傷を受けてもその奥の不変な真皮から同じ指紋が復元されるため、精密な個人の同定を可能にするバイオメトリクスとして広く知られている。

【０００５】

例えば、アクセスを要求する者がいる場合のユーザ認証動作においては、指紋を入力させることで、これが登録してある指紋と一致する場合にはアクセスを許可し、その指紋が一致していない場合には不正ユーザとしてアクセスを許可しないという使い方ができる。

【０００６】

所持品による認証ではそれを拾った他人が使用することができ、また知識でも盗み見たり、あるいは当て推量したりした者がその知識を入力することで、不正なアクセス許可を得ることができるのに比べ、バイオメトリクスによる方法では本当の本人だけが認証を受けられるという機能を実現している。

【０００７】

上記のような技術の例としては、特開平４－３３０６５号公報等に記載された技術がある。

【０００８】

【発明が解決しようとする課題】

上述した従来のユーザ認証方法では、バイオメトリクス、例えば指紋を入力し登録してある照合特徴と比較して本人確認をする方式の場合、指の乾燥や傷等で指紋画像の品質が悪くなると、登録や照合が成功しないユーザの存在を無視することができない。

【０００９】

このような場合、他の認証手段、例えばパスワードの入力で代替する回避法が代表的である。すなわち、指紋を入力し、それが自動照合が可能な品質に達しない場合、指紋による自動認証はあきらめ、代替手段としてパスワードをキーボードから入力させるという方法である。しかしながら、上述したように、パスワー

ドは盗み見等で他人が容易になりすますことが可能であり、システム全体のセキュリティホールになるという問題がある。

【００１０】

もちろん、指紋が自動認証に適さない場合には他のバイオメトリクス、例えば虹彩による照合等を併用するということも考えられるが、この場合、カメラ等の虹彩画像の入力装置や安定した画像を得るための照明システム等の付加的な設置・運用コストが必要であり、コスト増大が避けられない。

【００１１】

そこで、本発明の目的は上記の問題点を解消し、指紋等のバイオメトリクス入力データの品質が悪くかつ照合に適さないユーザがいる場合でも、大幅な付加的ハードウェア導入によるコスト増を招くことなく、システム全体のセキュリティを高めることができるバイオメトリクスを用いるユーザ認証方法及びそれを用いるユーザ認証装置を提供することにある。

【００１２】

【課題を解決するための手段】

本発明によるバイオメトリクスを用いるユーザ認証装置は、個人に固有の生体特徴であるバイオメトリクスの照合でユーザを認証するバイオメトリクスを用いるユーザ認証装置であって、前記バイオメトリクスの照合で認証不可の時に当該認証を要求したユーザのバイオメトリクスデータを取得する取得手段と、前記取得手段で当該バイオメトリクスデータが取得された時に前記バイオメトリクスの照合を代替する代替認証手段とを備えている。

【００１３】

本発明によるバイオメトリクスを用いるユーザ認証方法は、個人に固有の生体特徴であるバイオメトリクスの照合でユーザを認証するバイオメトリクスを用いるユーザ認証方法であって、前記バイオメトリクスの照合で認証不可の時に当該認証を要求したユーザのバイオメトリクスデータを取得するステップと、当該バイオメトリクスデータが取得された時に前記バイオメトリクスの照合を代替する代替認証手段で代替認証を行うステップとを備えている。

【００１４】

すなわち、本発明のバイオメトリクスを用いるユーザ認証方法は、バイオメトリクス照合によってユーザを認証する方法において、そのバイオメトリクス照合以外の代替認証手段を提供する際に、認証を要求したユーザのバイオメトリクスデータを取得することを特徴としている。

【００１５】

この場合、本発明のユーザ認証方法では、バイオメトリクス照合を目的として入力されたバイオメトリクスデータについて、自動照合に適した品質であるか否かを判定し、自動照合に適した品質でない場合に、取得したバイオメトリクスデータを保存するようにしている。

【００１６】

また、自動照合に適した品質でない場合には、入力されたバイオメトリクスが不正利用者探索・追跡に用いるのに適した品質であるか否かを判定し、適した品質である場合に限り、そのバイオメトリクス照合以外の代替認証手段を提供し、その代替認証手段を提供する際に取得したバイオメトリクスデータを保存しておき、それを不正利用者探索・追跡に用いるようにしている。

【００１７】

上記の不正利用者探索・追跡に用いるに適した品質であるか否かを決定する場合には、入力されるバイオメトリクスデータが正しくかつそのユーザがその場で入力したものであるか否かの判断を用いるようにしている。

【００１８】

さらに、本発明のユーザ認証方法では、ユーザにバイオメトリクス入力を複数回行わせ、複数回の入力によって得られたバイオメトリクスデータの相関を計測することで、そのユーザがその場で入力したものであるか否かの判断を行うようにしている。

【００１９】

本発明のユーザ認証方法では、バイオメトリクスとして指紋を用い、入力された画像が指紋と判断される画像であるか否かを、入力される指紋データが正しくかつそのユーザがその場で入力したものであるか否かの判断に用いている。

【００２０】

これによって、入門管理やコンピュータシステムへの不正ログインが実行されたことが後に判明した際に、その不正なりすましの実行者を特定することが可能となるので、指紋等のバイオメトリクス入力データの品質が悪くかつ照合に適さないユーザがいる場合でも、大幅な付加的ハードウェア導入によるコスト増を招くことなく、システム全体のセキュリティを高めることが可能となる。

【００２１】

【発明の実施の形態】

次に、本発明の実施例について図面を参照して説明する。図１は本発明の一実施例によるユーザ認証装置の構成を示すブロック図である。ここで、本発明の一実施例ではバイオメトリクスとして指紋を用いた例を示しており、図中の破線は処理手順（制御）の流れを、実線は指紋データ等のデータの流れを示している。

【００２２】

図１において、本発明の一実施例によるユーザ認証装置はユーザ情報入力部１０と、指紋入力部１１と、指紋照合用特徴抽出部１２と、指紋照合用登録特徴データ保存部１３と、指紋特徴照合部１４と、ユーザ認証結果決定部１５と、指紋入力要求部２０と、指紋入力部２１と、パスワード入力による代替認証部（以下、代替認証部とする）２２と、代替認証手段利用者情報保存部２３と、サービス許可または拒否表示部（以下、表示部とする）２４と、不正利用者追跡用情報処理部２５とから構成されている。

【００２３】

図２及び図３は本発明の一実施例によるユーザ認証装置の動作を示すフローチャートである。これら図１～図３を参照して本発明の一実施例によるユーザ認証装置の動作について説明する。尚、図２及び図３に示す処理動作は本発明の一実施例によるユーザ認証装置の各部が図示せぬ制御メモリのプログラムを実行することで実現可能であり、制御メモリとしてはＲＯＭ（リードオンリメモリ）やＩＣ（集積回路）メモリ等が使用可能である。

【００２４】

ユーザ情報入力部１０からはサービスの提供を求めるために認証を要求するユーザのユーザ名が入力される（図２ステップＳ１）。ユーザ名の入力においては

テンキーからユーザ番号を、あるいはキーボードからユーザ識別子を入力する他に、磁気方式のＩＤ（Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　ｎｕｍｂｅｒ）カード等を用いて入力することもできる。

【００２５】

指紋入力部１１ではそのユーザの指紋画像を入力するために、指紋センサ（図示せず）にユーザの指が接触した際にその指紋画像を撮影し、その画像データを処理可能なようにディジタル画像データに変換する（図２ステップＳ２）。

【００２６】

指紋センサの構成法としては、例えばＬＥＤ（Ｌｉｇｈｔ　Ｅｍｉｔｔｉｎｇ　Ｄｉｏｄｅ）で発せられた光をプリズムで反射し、この時、反射面の外側に置かれた指の隆線にしたがって隆起部と谷部とで反射率が異なることを利用し、ＣＣＤ（Ｃｈａｒｇｅ　Ｃｏｕｐｌｅｄ　Ｄｅｖｉｃｅ）を用いて反射光をディジタル画像化することで指紋画像を撮影する光学方式を用いることができる。

【００２７】

指紋照合用特徴抽出部１２では指紋入力部１１から得られた指紋画像を受取り、ここから指紋の識別に用いる特徴を抽出する処理を実行する（図２ステップＳ４）。

【００２８】

指紋の識別に用いる特徴抽出の実現法としては、例えば「マニューシャネットワーク特徴による自動指紋照合－－特徴抽出過程－－」（浅井紘、星野幸夫、木地和夫著、電子情報通信学会論文誌、ｖｏｌ．Ｊ７２－Ｄ－ＩＩ、ｎｏ．５、ページ７２４～７３２、１９８９年５月）に記述された方法がある。

【００２９】

ここでは隆線を含む濃淡画像から二値化処理・細線化処理によって隆線パターンを抽出し、隆線の端点と分岐点との位置を検出した後に、それら相互間を結ぶ線分上の交差隆線数を計数し、その関係図をディジタルデータ表現することによって、照合のための指紋特徴としている。

【００３０】

その際、付加的な情報として、指紋画像のうちの特徴抽出に十分な画像品質で

ある領域の面積、特徴抽出から得られた端点・分岐点等の特徴の数、自動特徴抽出処理が各特徴に付与した信頼度情報情報等も計算される。

【００３１】

さらに、指紋照合用特徴抽出部１２ではこの特徴抽出の結果に基づき、入力された指紋が自動指紋照合を用いた認証に適した品質であるか否かを判定する（図２ステップＳ５）。自動指紋照合が可能であるためには、指紋の隆線とその間の谷とのなす凹凸のコントラストが大きくいことが必要であるが、皮膚の乾燥や・発汗や傷・摩耗等によって必要な品質で指紋画像を得られない場合があり、このような場合は不十分な品質と判定することになる。

【００３２】

この判定部の実現法としては、例えば指紋照合用特徴抽出部１２で得られた特徴抽出に十分な画像品質である領域の面積、特徴抽出から得られた端点・分岐点等の特徴毎の数、自動特徴抽出処理が各特徴に付与した信頼度情報情報等がそれぞれあるいはそれらの組合せが予め定められた閾値以上であるか否かを判定することで実現する方法がある。

【００３３】

指紋照合用登録特徴データ保存部１３は照合用の指紋特徴情報と、その指紋の持ち主であるユーザに関する情報とを互いに対応させて記憶しておく部分である。ここでいうユーザ固有情報とは、ユーザを識別し、そのユーザに許可するサービスの種別・範囲等である。

【００３４】

指紋照合用特徴抽出部１２において十分な品質であると判定された場合、指紋特徴照合部１４はそのユーザについての登録特徴と入力指紋の特徴とが一致する（十分近似する）かどうかが照合する（図２ステップＳ６）。

【００３５】

指紋特徴照合部１４は今回ユーザが入力した指紋から求めた指紋特徴Ｓを指紋照合用特徴抽出部１２から、一方これまでに記憶させられている指紋特徴情報の中からユーザ情報として入力されたユーザ名に対応する指紋特徴情報Ｆを指紋照合用登録特徴データ保存部１３からそれぞれ入力し、指紋特徴情報Ｆと指紋特徴

Ｓとを比較し、それらの情報が同一の指から得られたものである時に高くなるような、類似性に応じたスコアを評価する。

【００３６】

指紋特徴照合部１４はこのスコアを予め設定された閾値と比較することで、その指紋情報Ｓを与えたユーザが登録されたユーザと同一であるか否かを判定し（図２ステップＳ７）、これが閾値より高い場合に「指紋は一致」という識別結果を出力する。

【００３７】

このような指紋を使った押捺者識別のための照合の実現法としては、例えば「マニューシャネットワーク特徴による自動指紋照合－－照合過程－－」（淺井紘、星野幸夫、木地和夫著、電子情報通信学会論文誌、ｖｏｌ．Ｊ７２－Ｄ－ＩＩ、ｎｏ．５、ページ７３３～７４０、１９８９年５月）に記述された方法がある。

【００３８】

ここでは隆線の端点と分岐点との相互間を結ぶ線分上の交差隆線数を計数してディジタルデータ表現したもの同士で位置合せを行い、その後にそれらの間の類似性を評価することによって照合を実現している。

【００３９】

指紋照合の結果、入力された指紋がそのユーザについて記憶された指紋特徴と十分に近似していた場合、ユーザ認証結果決定部１５はそのユーザ情報を入力したユーザを正規のユーザと認証し、サービスが許可される旨を表示部２４に表示することとなる（図２ステップＳ８）。一方、指紋が一致しない場合、認証不成功としてサービスは拒否されるとともに、代替認証を行うために、指紋入力要求部２０に進むことになる。

【００４０】

上述した処理動作は、指紋照合用特徴抽出部１２において自動照合を行うのに品質が十分であると判定された場合である。一方、指紋照合用特徴抽出部１２において不十分であると判定された場合、あるいはユーザ認証結果決定部１５において入力された指紋での認証が不成功となった場合、指紋入力要求部２０からユ

ーザに対して複数回の指紋センサへの指紋入力が要求される（図３ステップＳ９～Ｓ１１）。ここで、複数回の指紋入力を要求しているのは、これによって偽造した指紋の入力を発見して排除するためである。

【００４１】

指紋入力部２１は指紋入力部１１と同様の仕組みによって指紋画像の入力、取得を行う。指紋入力要求部２０の要求にしたがって指紋入力部２１から必要な指紋入力が実行された場合に限り、ユーザは代替認証部２２での代替認証のステップに進むことができる（図３ステップＳ１２）。

【００４２】

代替認証部２２での代替認証方法としては、例えばテンキーやキーボードからの暗証番号やパスワードの入力、保持者を照明する磁気カードの読込み等の方法が考えられる。これらの代替認証方法によって正当なユーザであると判断された場合（図３ステップＳ１３）、上記のバイオメトリクス自動照合によって認証された場合と同様に、そのユーザ情報を入力したユーザは正規のユーザと認証され、サービスが許可される旨が表示部２４に表示されることとなる（図３ステップＳ１４）。それ以外の場合には、認証不成功としてサービスが拒否される旨が表示部２４に表示されることとなる（図３ステップＳ１５）。

【００４３】

代替認証手段利用者情報保存部２３は最初に指紋入力部１１から入力された画像及び指紋入力要求部２０で要求された後に指紋入力部２１から入力された画像を保存する（図２ステップＳ３及び図３ステップＳ１０）。この保存された画像は、後に必要に応じて、不正利用者追跡用情報処理部２５で不正利用者の探索・追跡に使用される。

【００４４】

図４は本発明の他の実施例によるユーザ認証装置の構成を示すブロック図である。図４において、本発明の他の実施例によるユーザ認証装置は入力画像正当性判定部２６を設けた以外は図１に示す本発明の一実施例によるユーザ認証装置と同様の構成となっており、同一構成要素には同一符号を付してある。また、同一構成要素の動作は本発明の一実施例と同様である。

【００４５】

図５及び図６は本発明の他の実施例によるユーザ認証装置の動作を示すフローチャートである。これら図４～図６を参照して本発明の他の実施例によるユーザ認証装置の動作について説明する。尚、図５及び図６に示す処理動作は本発明の他の実施例によるユーザ認証装置の各部が図示せぬ制御メモリのプログラムを実行することで実現可能であり、制御メモリとしてはＲＯＭやＩＣメモリ等が使用可能である。

【００４６】

また、図５及び図６に示す処理動作のうちのステップＳ２１～Ｓ３０，Ｓ３４～Ｓ３７の動作は図２のステップＳ１～Ｓ８及び図３のステップＳ９～Ｓ１５の動作と同様であるので、以下、本発明の他の実施例によるユーザ認証装置の特徴的な動作について説明する。

【００４７】

本発明の他の実施例によるユーザ認証装置では、本発明の一実施例と同様に、ユーザ認証結果決定部１５において入力された指紋での認証が不成功となり、代替認証部２２での代替認証が必要となった場合、指紋入力要求部２０からユーザに対して指紋センサへの指紋入力が要求され、指紋入力部２１で指紋画像が取得される（図６ステップＳ２９）。

【００４８】

入力画像正当性判定部２６は入力センサから入力される指紋画像が、現在、サービスのための認証を要求しているユーザの正しく提示した指の指紋の画像であるか否かを判定する（図６ステップＳ３０，Ｓ３１）。

【００４９】

この判定において排除すべきは次のようなケースである。（１）このユーザが指紋でない生体物、例えば指の指紋以外の部分、手のひらの一部、その他の皮膚の部分等を提示しているケース、（２）生体でないが指紋に似せたもの、例えばゴムやシリコン等の人体に似た材質で指を模して作り、しかも表面に他人の指紋を添付したものを提示しているケース等である。

【００５０】

入力画像正当性判定部２６では上記のような偽指による画像提示を排除するため、まずその画像の指紋らしさを評価し、これが閾値以上であることを判定の条件とする。指紋らしさの評価には画像を小領域に分割し、それぞれについて２次元フーリエ変換等によって周波数分布を調べる方法を用いる。

【００５１】

人間の指紋における隆線はある程度限られたピッチ分布を持つ縞模様をなしており、周波数分布においてピークの分布を評価することによって、これを確認することができる。指紋の一部において傷・乾燥等で自動照合に適さないような品質であっても、指紋ならば縞模様を観察することができる領域は広いはずであり、この方法で指紋と他の部分とを区別することができる。

【００５２】

また、提示されたものが生体の指であることを確認するためには、複数の入力画像間の類似度を調べる方法を用いる。人間の指は弾性があり、押捺の度毎に指の変形の仕方は微妙に異なる可能性が高く、複数の押捺画像が細部まで一致する場合、それらは生体の指とは弾性の異なる模倣物（レプリカ）が提示され、正しい押捺でないと判断するのが妥当である。

【００５３】

したがって、複数回の指紋画像の間で、平行移動・回転によって位置合せをして隆線パターンの位置的相関性がかなり高くなったとすれば、それらの画像の元はある程度の剛性を持つ物体と考えることができ、この程度を評価することによって、弾力性を持ち、押捺の度に必然的に異なる歪み方をするはずの指の皮膚との分別を行うことができる。

【００５４】

さらに、入力センサにおいて、指の押捺入力が始まってから押捺面積が広くなり、再び狭くなって押捺を修了するまでの動画像を撮影し、得られた時間方向の画像系列からこの時の指の弾性による変形の程度を評価し、指の弾力性に合わない入力を分別することができる。さらにまた、指紋画像における汗腺孔の有無を調べる方法を用いることもできる。汗腺孔は隆線上において、ごく微細な構造を持つため、レプリカにおいて加工、複製することがかなり困難であると考えられ

る。

【００５５】

入力画像正当性判定部２６における上記のような判定によって、入力画像が正当な指紋の入力であると判断された場合に限り、ユーザは代替認証部２２での代替認証のステップに進むことができる。

【００５６】

代替認証部２２での代替認証方法としては、例えばテンキーやキーボードからの暗証番号やパスワードの入力、保持者を照明する磁気カードの読込み等の方法がある。これらの代替認証方法によって正当なユーザであると判断された場合には、上記のバイオメトリクス自動照合によって認証された場合と同様に、そのユーザ情報を入力したユーザが正規のユーザと認証され、サービスが許可されることになり、それ以外の場合には認証不成功としてサービスが拒否される。

【００５７】

代替認証手段利用者情報保存部２３は指紋入力要求部２０で要求された後に入力された画像を保存する（図６ステップＳ３０）。この保存された画像は、後に必要に応じて、不正利用者追跡用情報処理部２５で不正利用者の探索・追跡に使用される。

【００５８】

以上、本発明の一実施例及び他の実施例の各部の構成及び動作について説明したが、以下、その使用例について説明する。本発明は、例えば重要施設の入室ゲートの通過者管理（物理アクセスコントロール）や、重要な情報を含むコンピュータシステムへのログイン管理等に用いられる。

【００５９】

例えば、物理アクセスコントロール応用における動作例としては、入門を要求するユーザがテンキー等から自分を識別する番号Ｎ等を入力するとともに、指紋センサから指紋Ｓを入力する。システムは記憶されている複数の登録指紋の中で入力されたユーザの識別番号Ｎで区別される指紋Ｆと指紋Ｓとの一致を判別する。実際の照合では指紋Ｓ及び指紋Ｆそれぞれから抽出された照合用の特徴同士の類似度が評価され、閾値以上であれば一致と判定することになる。

【００６０】

これらの照合処理は自動で行われるわけであり、入力される指紋の品質が十分でない場合、十分な確信をもって同一指か否かの判定を行えないことになる。ユーザがそのような低品質な指紋を入力した場合、従来は、上述したように、「自動照合処理による認証不能」と判定し、代替手段として特別な暗証番号あるいはパスワードの入力を要求し、それが予め登録してあるものと一致すれば認証成功とするという方法が一般的である。

【００６１】

本システムでは入力された指紋の画像品質が不十分なために自動照合が成功しなかった場合、この最初に入力された指紋画像を代替認証手段利用者情報保存部２３に保存するとともに、代替認証を許可するに先立って、重ねての指紋入力を要求する。

【００６２】

このように、複数回の指紋入力を要求するのは、上述したように、複数の指紋画像を互いに比較し、あるいは指紋押捺を記録する動画像から得た時系列画像を利用することによって、偽指の画像を与えられそのまま保存するのを防ぐためである。入力された複数の画像、または時系列の画像の正当性を入力画像正当性判定部２６で判定し、もしそれらが生体の指紋でない場合には代替認証を許可しないことになる。

【００６３】

入力される画像が正当なものである場合は、それは代替認証手段利用者情報保存部２３に保存され、パスワード入力による代替認証部２２での代替認証に進める。入力するパスワードあるいは暗証番号が予め登録されているものと一致すれば正しく認証されたものとし、ユーザはサービスを受けることができる。

【００６４】

代替認証のためにテンキー、キーボード等から入力するパスワードあるいは暗証番号は推量、盗み見等によって他人でも打ち込むことが可能であり、正しいユーザになりすました不正アクセスの可能性が生じることになる。本システムでは、入門ゲート管理やコンピュータシステムへの不正ログインが実行されたことが

後に判明した際に、その不正なりすましの実行者を特定する手段を提供する。

【００６５】

すなわち、代替認証手段利用者情報保存部２３に保存されている画像は代替認証部２２を利用したユーザの指紋情報を含んでおり、これを管理者等が目視することによって、不正利用者の探索・追跡に役立てることができる。多くの場合、このようなシステムの利用者の範囲は限られているため、各自の指紋と保存されている画像を目視で比べることによって、追跡のための多くの情報を得ることができ、不正利用者の発見や追求に役立てることができる。

【００６６】

尚、上述した説明では、バイオメトリクスデータとして１本の指の指紋を用いる方法を説明したが、もちろん複数の指を入力し、それらを用いて入力画像の正当性（正しくユーザが生きた指を提示しているか）をより厳密に判定し、また複数の指についての指紋画像を保存しておいて不正利用者追跡に用いることで、よりセキュリティを高めることもできる。

【００６７】

また、指紋入力に先立って、ユーザ情報入力部１０からユーザ識別情報を入力する例を示しているが、これは必ずしも必須ではない。ユーザ識別情報を入力せずに指紋入力１１を行った場合、そこから特徴抽出を行い、得られた特徴を指紋特徴照合部１４において、指紋照合用登録特徴データ保存部１３に保存されたすべての指紋特徴データと順に照合し、もっとも類似度スコアが高い指紋について、その登録ユーザに提供されるべきサービスを許可すればよいことになる。

【００６８】

本発明の一実施例及び他の実施例ではバイオメトリクスの一例として指紋の場合を挙げて説明しているが、指紋センサを、自動照合の部分を別のバイオメトリクス（個人に固有の生体特徴）を入力し、特徴を抽出して照合する手段で置換すれば、掌紋、顔、虹彩、網膜血管パターン、掌形、筆跡、声紋等の他のバイオメトリクスを使用することも可能である。

【００６９】

また、通常のバイオメトリクス認証では指紋を用い、代替認証に先立ってのバ

イオメトリクスデータ保存では他のバイオメトリクスを用い、あるいは併用することもできる。例としては、代替認証の際に顔画像を撮影する、あるいは指紋入力する姿を撮影する等である。指紋入力の過程を別のカメラで撮影することは、入力画像正当性判定部２６において正しく指紋を入力しているかどうかの正当性判定に利用可能であるとともに、後の不正利用者追跡用処理において効果を発揮する情報を保存する有効な方法である。

【００７０】

このように、認証に対する脅威となる、他人になりすましてのサービス要求によるシステム攻撃者を探す場合、代替認証者については保存しておいた指紋画像が使用することができる。

【００７１】

これらはログイン時の自動照合には不十分な品質であっても、人手での攻撃者探索に役立つような情報を提供する。入力画像正当性判定部２６で偽指によるごまかしは排除されるので、画像は攻撃者本人の指に関する手がかり・証拠を示すことになる。また、パスワードを入力するにも自分の指紋画像を要求されることはなりすまし攻撃への抑止効果をも持ち、システム全体のセキュリティ向上に役立つ。

【００７２】

【発明の効果】

以上説明したように本発明によれば、個人に固有の生体特徴であるバイオメトリクスの照合でユーザを認証するバイオメトリクスを用いるユーザ認証装置において、バイオメトリクスの照合で認証不可の時に当該認証を要求したユーザのバイオメトリクスデータを取得し、その取得後にバイオメトリクスの照合を代替することによって、指紋等のバイオメトリクス入力データの品質が悪くかつ照合に適さないユーザがいる場合でも、大幅な付加的ハードウェア導入によるコスト増を招くことなく、システム全体のセキュリティを高めることができるという効果がある。

【図面の簡単な説明】

【図１】

本発明の一実施例によるユーザ認証装置の構成を示すブロック図である。

【図２】

本発明の一実施例によるユーザ認証装置の動作を示すフローチャートである。

【図３】

本発明の一実施例によるユーザ認証装置の動作を示すフローチャートである。

【図４】

本発明の他の実施例によるユーザ認証装置の構成を示すブロック図である。

【図５】

本発明の他の実施例によるユーザ認証装置の動作を示すフローチャートである。

【図６】

本発明の他の実施例によるユーザ認証装置の動作を示すフローチャートである。

【符号の説明】

１０　ユーザ情報入力部

１１　指紋入力部

１２　指紋照合用特徴抽出部

１３　指紋照合用登録特徴データ保存部

１４　指紋特徴照合部

１５　ユーザ認証結果決定部

２０　指紋入力要求部

２１　指紋入力部

２２　パスワード入力による代替認証部

２３　代替認証手段利用者情報保存部

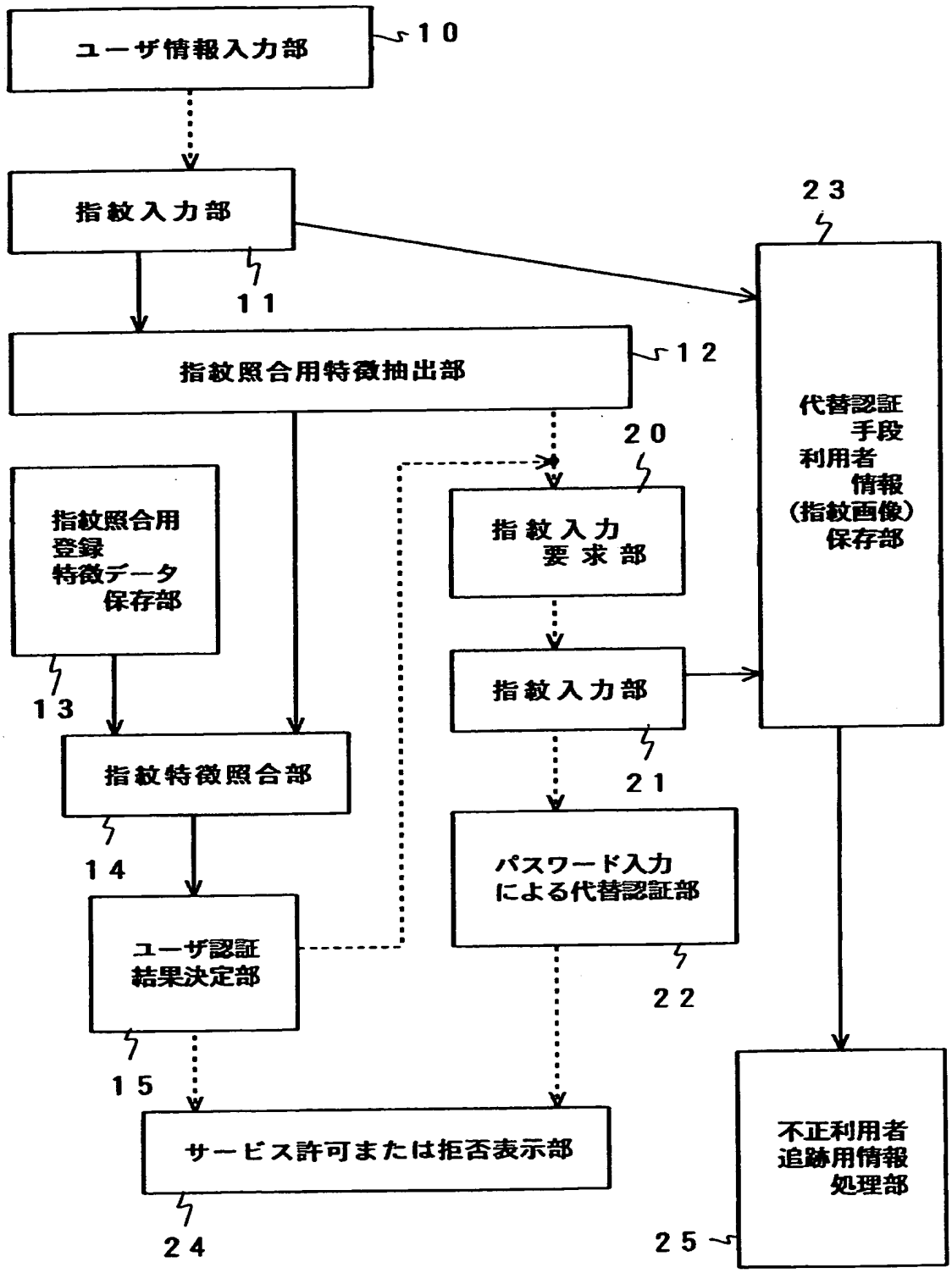
２４　サービス許可または拒否表示部

２５　不正利用者追跡用情報処理部

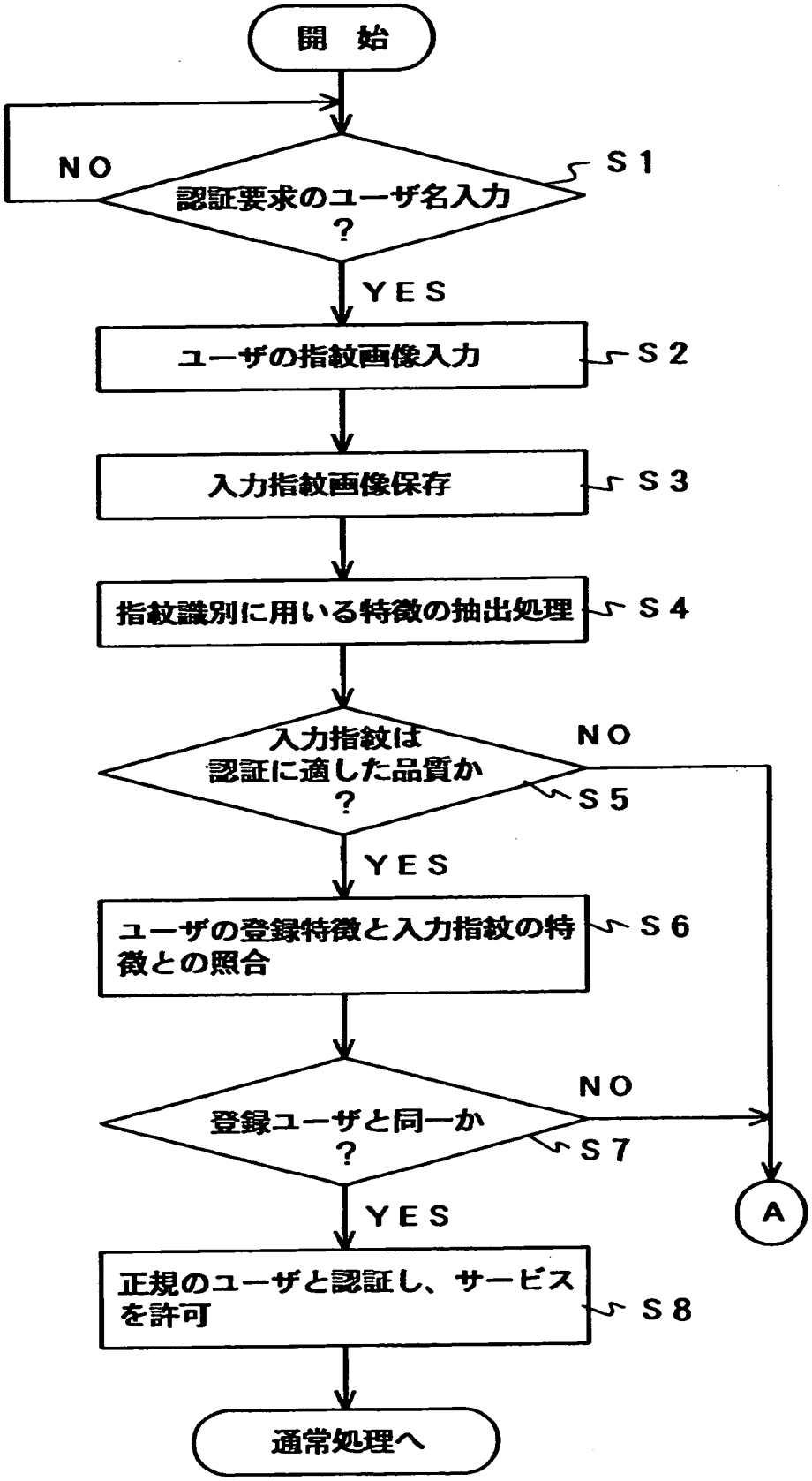
２６　入力画像正当性判定部

【書類名】　　図面

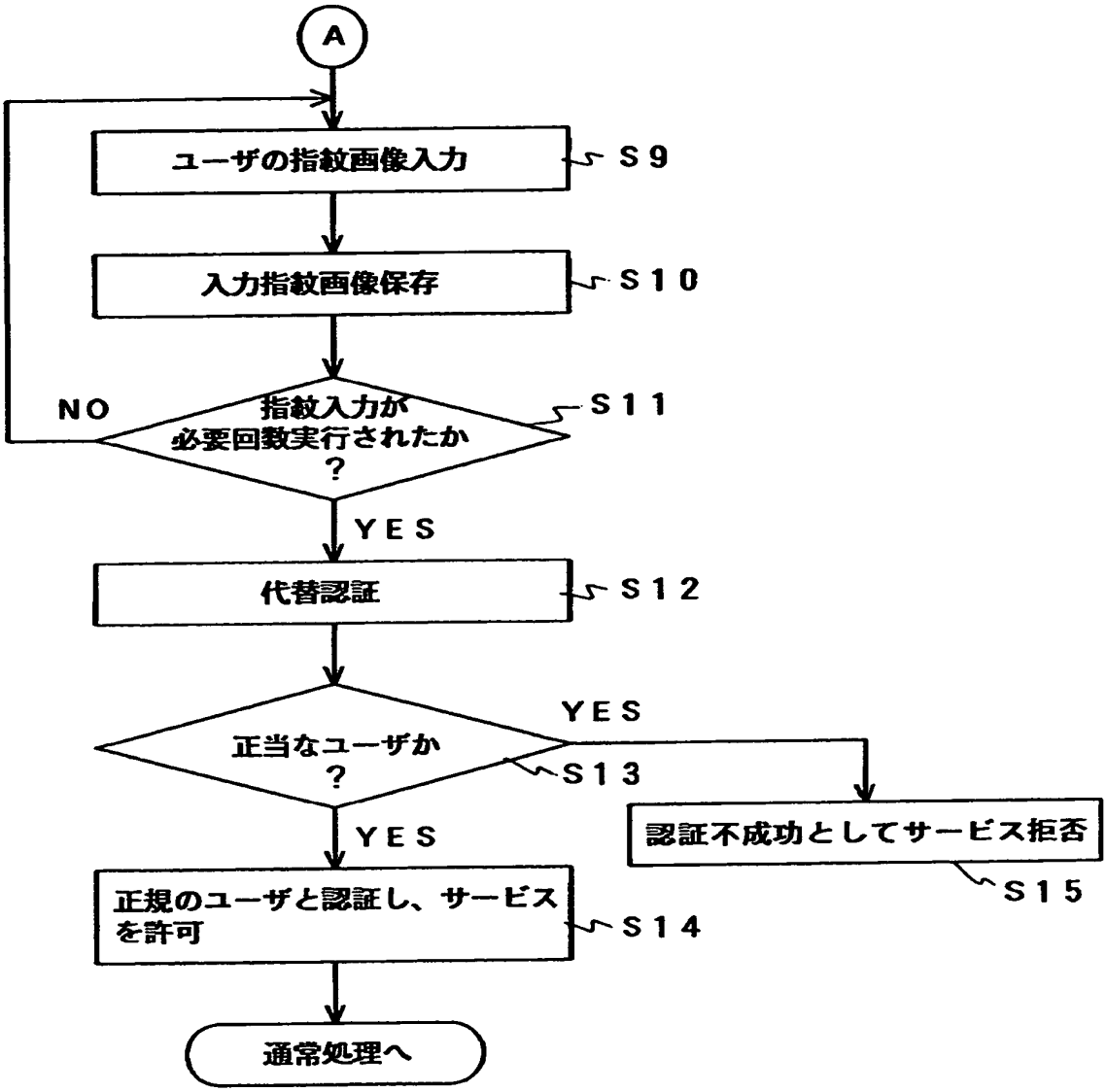
【図１】


ユーザ情報入力部
10
指紋入力部
11
23
指紋照合用特徴抽出部
12
代替認証
手段
利用者
情報
(指紋画像)
保存部
20
指紋照合用
登録
特徴データ
保存部
指紋入力
要求部
13
指紋入力部
指紋特徴照合部
21
14
パスワード入力
による代替認証部
ユーザ認証
結果決定部
22
15
サービス許可または拒否表示部
不正利用者
追跡用情報
処理部
24
25

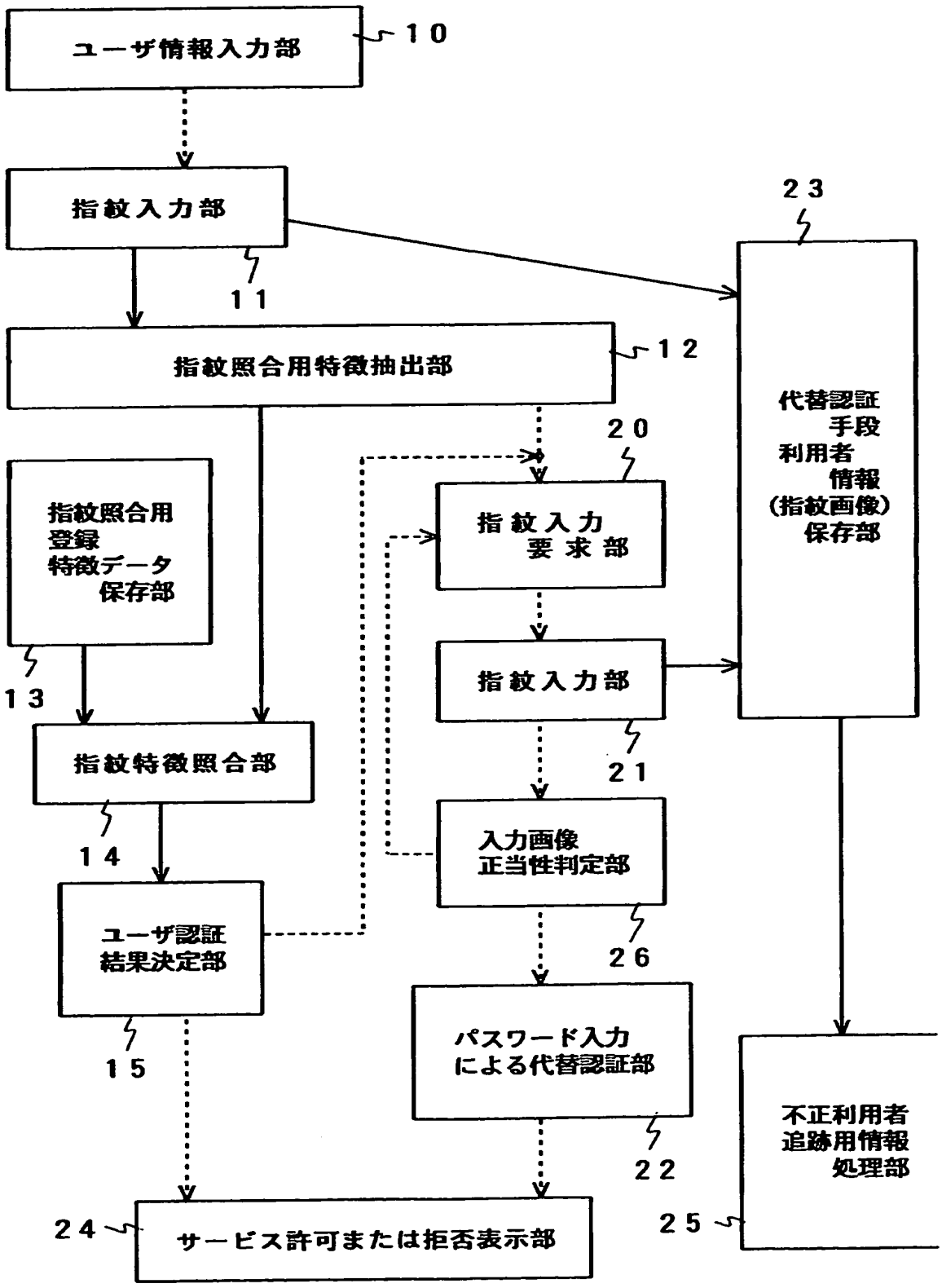
【図２】


開　始
NO
認証要求のユーザ名入力？
S１
YES
ユーザの指紋画像入力
S２
入力指紋画像保存
S３
指紋識別に用いる特徴の抽出処理
S４
入力指紋は認証に適した品質か？
NO
S５
YES
ユーザの登録特徴と入力指紋の特徴との照合
S６
登録ユーザと同一か？
NO
S７
YES
A
正規のユーザと認証し、サービスを許可
S８
通常処理へ

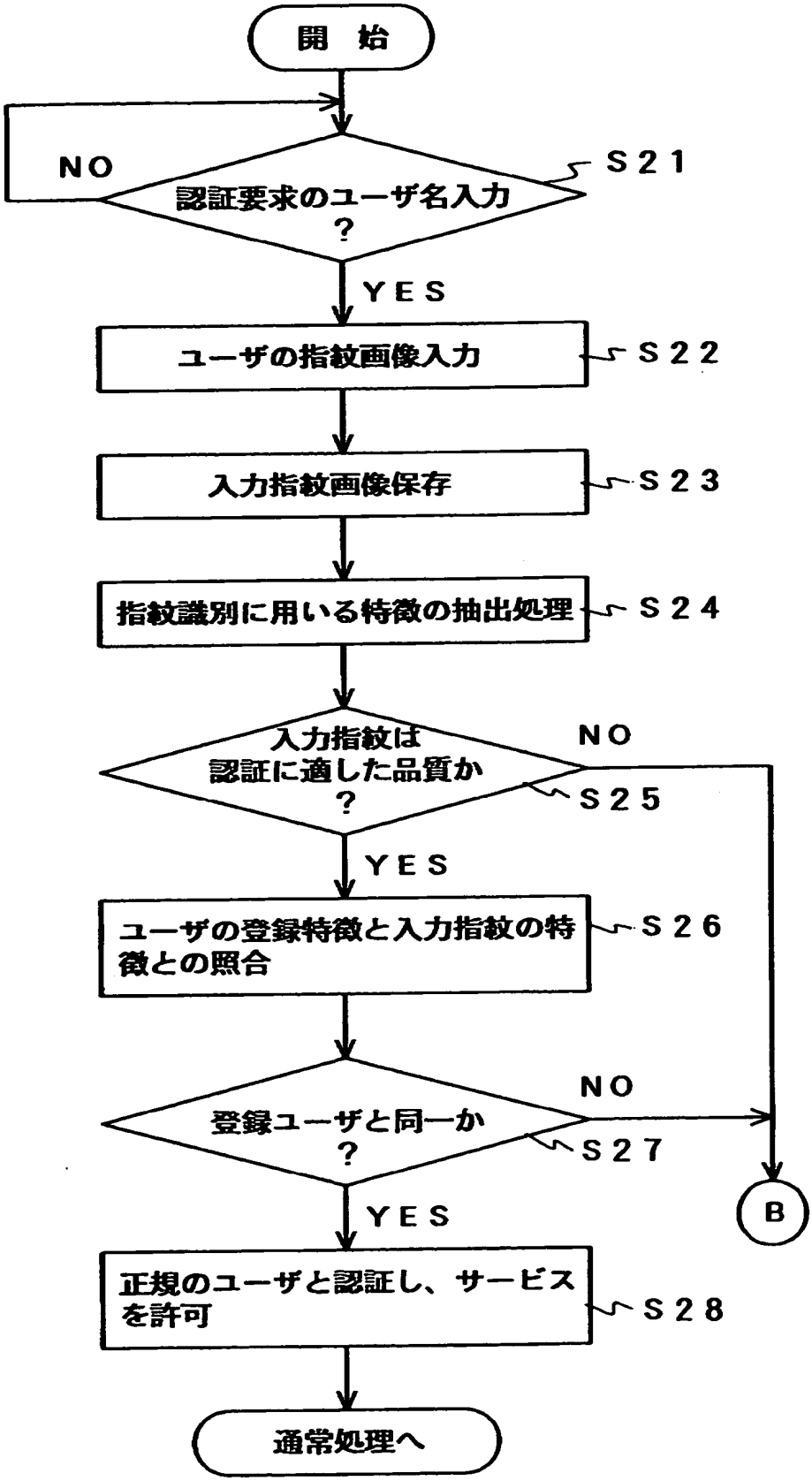
【図３】


A
ユーザの指紋画像入力
S９
入力指紋画像保存
S１０
NO
指紋入力が必要回数実行されたか？
S１１
YES
代替認証
S１２
正当なユーザか？
YES
S１３
YES
認証不成功としてサービス拒否
S１５
正規のユーザと認証し、サービスを許可
S１４
通常処理へ

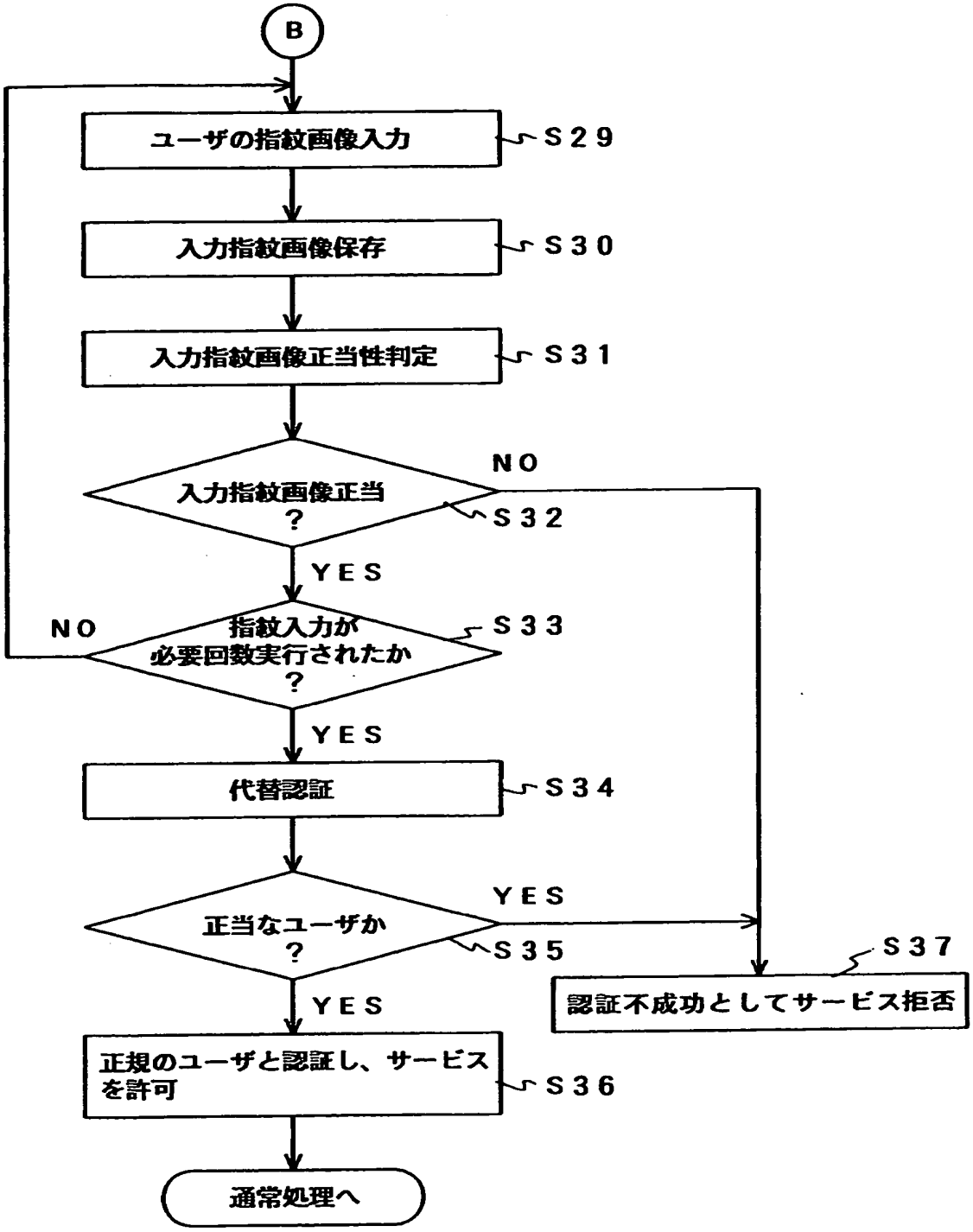
【図４】


ユーザ情報入力部
10
指紋入力部
11
23
指紋照合用特徴抽出部
12
代替認証手段利用者情報（指紋画像）保存部
20
指紋照合用登録特徴データ保存部
指紋入力要求部
13
指紋入力部
指紋特徴照合部
21
14
入力画像正当性判定部
ユーザ認証結果決定部
26
パスワード入力による代替認証部
不正利用者追跡用情報処理部
15
22
24
サービス許可または拒否表示部
25

【図５】


開　始
NO
認証要求のユーザ名入力？
S２１
YES
ユーザの指紋画像入力
S２２
入力指紋画像保存
S２３
指紋識別に用いる特徴の抽出処理
S２４
入力指紋は認証に適した品質か？
NO
S２５
YES
ユーザの登録特徴と入力指紋の特徴との照合
S２６
登録ユーザと同一か？
NO
S２７
YES
B
正規のユーザと認証し、サービスを許可
S２８
通常処理へ

【図６】


B
ユーザの指紋画像入力
S29
入力指紋画像保存
S30
入力指紋画像正当性判定
S31
入力指紋画像正当？
NO
S32
YES
指紋入力が必要回数実行されたか？
NO
S33
YES
代替認証
S34
正当なユーザか？
YES
S35
YES
正規のユーザと認証し、サービスを許可
S36
通常処理へ
S37
認証不成功としてサービス拒否

【書類名】　　要約書

【要約】

【課題】　指紋等のバイオメトリクス入力データの品質が悪くかつ照合に適さないユーザがいる場合でも、大幅な付加的ハードウェア導入によるコスト増を招くことなく、システム全体のセキュリティを高めることが可能なユーザ認証装置を提供する。

【解決手段】　指紋照合用特徴抽出部１２において不十分であると判定された場合、ユーザ認証結果決定部１５において入力された指紋での認証が不成功となった場合、指紋入力要求部２０からユーザに対して指紋入力が要求される。指紋入力部２１から必要な指紋入力が実行された場合、代替認証部２２での代替認証が許可される。代替認証部２２での代替認証の結果に応じてサービス許可または拒否表示部２４にその旨が表示される。代替認証手段利用者情報保存部２３には指紋入力部１１または指紋入力部２１から入力された画像が保存される。

【選択図】　　図１

出 願 人 履 歴 情 報

識別番号　〔０００００４２３７〕

１．変更年月日　１９９０年　８月２９日
［変更理由］　新規登録
住　所　東京都港区芝五丁目７番１号
氏　名　日本電気株式会社